УДК 327.8

А. А. Муратова
Уральский федеральный университет,
Екатеринбург

Республика Корея в условиях цифровых угроз

XXI в. стал веком прорывных информационных технологий, которые привнесли в жизнь современного общества как новые возможности развития, так и новые проблемы и угрозы. Развитые информационные технологии изменили стиль жизни общества, соответственно, и общественные ценности. Одним из основных последствий глобальной информатизации государственных и военных структур стало возникновение новой среды – киберпространства [1].

По мере увеличения числа пользователей Интернета возрастают угрозы в сфере кибербезопасности, связанные с нарушением конфиденциальности и утечкой персональных данных [2]. Неправомерное использование информационно-коммуникационных технологий (ИКТ) ведет к появлению таких угроз, как возможность манипулирования информацией частных лиц или других государств; дезинформация и сокрытие информации; искажение традиционных культурных, нравственных, этических и эстетических ценностей [3].

По данным комиссии ООН, лидером по уровню проникновения широкополосного Интернета стала Республика Корея – 98,8 % [4]. Страна сталкивается с угрозой внешних кибератак, что вынуждает ее концентрировать все усилия на защите своего киберпространства. Правительственные организации и финансовые фирмы стали зависимыми от веб-сайтов и веб-приложений, следовательно, они более подвержены кибератакам [5].

Одна из самых масштабных кибератак последних лет в Республике Корея произошла 20 марта 2013 г. Согласно отчету Корейского агентства по интернет-безопасности (KISA), в Республике Корея атакам типа DDoS (отказ в обслуживании) подверглись 48 тыс. компьютеров. Экономический ущерб кибератаки был оценен в 750 млн долларов [6]. Вредоносное

программное обеспечение (ПО), в результате которого прекратили работу национальные корейские компьютерные сети на телевизионных станциях KBS, MBC, YTN, а также были прекращены операции в трех банках – *Shinhan, NongHyup* и *Jeju*, называется *DarkSeoul* [7].

Правительство Республики Корея заявило, что злоумышленники получили контроль над персональными компьютерами или серверными компьютерами в целевых организациях. После выполнения действий по мониторингу злоумышленники отправили команду на удаление данных, хранящихся на сервере, и распространили вредоносное ПО на отдельные компьютеры через центральный сервер [7].

Эксперты до сих по не могут выяснить, кто виноват в ряде кибератак, совершенных в отношении Южной Кореи. В Республике Корея эксперты по кибербезопасности связали инцидент с китайским IP-адресом, что усилило подозрения в отношении Северной Кореи, так как «эксперты по разведке считают, что Северная Корея обычно использует китайские компьютерные адреса, чтобы скрыть свои кибератаки» [8].

Из вышесказанного можно сделать вывод о том, что система обеспечения кибербезопасности Республики Корея нуждается в усовершенствовании. С развитием ИКТ растет и необходимость в проведении политики, регулирующей и ограничивающей деятельность в киберпространстве, так как сегодня мир очень зависим от бесперебойного функционирования информационной инфраструктуры, именно от ее работы зависит как моральное, так и материальное благосостояние людей, а иногда даже их жизнь.

Библиографические ссылки

1. *Бородакий Ю. В*. Кибербезопасность как основной фактор национальной и международной безопасности XXI века // Cyberleninka : [сайт]. URL: https://cyberleninka.ru/article/n/kiberbezopasnost-kak-osnovnoy-faktor-xxi-veka-chast (дата обращения: 23.09.2019).
2. 장인주, 유형선 개인정보보호 강화를 위한 동적 보안수준 결정 [Jang In Ju, *Yoo Hyong Son.* Dynamic Sensitivity Level Measurement for Privacy Protection] // Electronic Transactions. 2012. № 17 (1). P. 137–150.

3. *Казарин О. В.*, *Тарасов А. А*. Современные концепции кибербезопаснсти ведущих зарубежных государств // Cyberleninka : [сайт]. 2013. URL: https://cyberleninka.ru/article/n/sovremennye-kontseptsii-1 (дата обращения: 05.10.2019).
4. Южная Корея – лидер по уровню проникновения Интернета // MoSeoul : [сайт]. URL: http://mojseul.ru/obshhestvo/yuzhnaya-koreya-lider.html (дата обращения: 05.10.2019).
5. Cyberattacks // Akamai : [website]. URL: https://www.akamai.com/en/resources/cyber-attacks.jsp (accessed: 06.10.2019).
6. *Choi K.*, *Manicon J., Palamar S.* Mutual Securty in the Asia-Pacific: Roles for Australia, Canada and South Korea. McGill-Queen's Univ. Press, 2015 // JSTOR : [website]. URL: https://www.jstor.org/stable/j.ctt1jktr6v (accessed: 06.10.2019).
7. South Korea blames North for bank and TV cyber-attacks // BBC News : [website]. 10.04.2013. URL: https://www.bbc.com/news/technology-22092051 (accessed: 01.10.2019).
8. China IP address link to South Korea cyber-attack // BBC News : [website]. 10.04.2013. URL: https://www.bbc.com/news/world-asia-21873017 (accessed: 05.10.2019).